

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

7



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
 United States Patent and Trademark Office
 Address: COMMISSIONER FOR PATENTS
 P.O. Box 1450
 Alexandria, Virginia 22313-1450
 www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/511,751	02/24/2000	Boby Joseph	99,815	5539
20306	7590	08/09/2004	EXAMINER	
MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP			LANIER, BENJAMIN E	
300 S. WACKER DRIVE			ART UNIT	PAPER NUMBER
32ND FLOOR			2132	
CHICAGO, IL 60606			DATE MAILED: 08/09/2004	

Please find below and/or attached an Office communication concerning this application or proceeding.

7

Office Action Summary	Application No.	Applicant(s)	
	09/511,751	JOSEPH ET AL.	
	Examiner	Art Unit	
	Benjamin E Lanier	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 02 June 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-36 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-10, 13-22, 25-28, 30-34, 36 is/are rejected.
- 7) ☒ Claim(s) 11, 12, 23, 24, 29 and 35 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 24 February 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s). _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

1. Applicant's amendment of claims 1, 13, 25-31 has been fully considered and is entered.

Response to Arguments

2. Applicant's arguments, see Amendment A, filed 2 June 2004, with respect to the rejection(s) of claim(s) 1, 2, 5, 8, 9, 13, 14, 17, 20, 21, 25, 26, 30-32 and 36 under 35 U.S.C. § 102(e) as being anticipated by Heer have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Pinder U.S. patent No. 6,105,134.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1, 2, 5, 8, 9, 13, 14, 17, 20, 21, 25, 26, 30-32, 36 are rejected under 35 U.S.C. 102(e) as being anticipated by Pinder, U.S. Patent No. 6,105,134. Referring to claims 1, 2, 5, 8, 13, 14, 17, 20, 25, 26, 30-32, 36, Pinder discloses a conditional access system wherein a service distribution organization (second network device) broadcasts an encrypted instance of the service. Encrypted instance is broadcast over a transmission

Art Unit: 2132

medium and is received in a large number of set top boxes (first network device, third network device), each of which is attached to a television set. Encrypted instance contains instance data, and entitlement control messages. It is a function of the set top box to determine whether the encrypted instance should be decrypted using the decryptor included in the set top box which uses a control word, which meets the limitation of key material, as a key to decrypt encrypted instance. The control word is produced by control word generator from information contained in entitlement control message and information from authorization information stored in the set top box. For example, authorization information may include a key (base key) for the service and an indication of what programs in the service the subscriber is entitled to watch (key extension). If the authorization information indicates that the subscriber is entitled to watch the program of encrypted instance, the control word generator uses the key together with the information from the entitlement control message (key extension) to generate control word, which meets the limitation of a first network device having a first set of key material (Col. 4, lines 14-59), the first set of key material including a first base key and a key extension in addition to the first base key, a second network device having the first set of key material and a second set of key material, the second key material including a second base key, wherein the second network device is capable of communicating with the first network device using security determined by the first set of key material. The authorization information used in a particular set top box is obtained from one or more entitlement management messages addressed to the set top box. Subscribers generally purchase services by the month or a one time event, and after a subscriber has purchased a service, the service distribution organization sends set entitlement management messages to the

Art Unit: 2132

set top box belonging to the subscriber as required for the purchased services (Col. 4, line 60 – Col. 5, line 10). The limitation of a third network device having the second set of key material, the third network device is capable of communicating with the second network device using security determined by the second set of key material is met by a set top box that is not authorized to watch a certain instance of the broadcast service and therefore would lack the particular portion of the authorization information that allows access to the broadcast instance once the control word is generated. Regarding the limitation of the security being determined by the first key material being stronger than the security being determined by the second set of key material is met by previously mentioned scenario where an authorized set top box would generate a control word with a higher security level than that of an set top box lacking authorization.

Referring to claims 9, 21, Pinder discloses that the set top box cryptographic key is generated based on the public key used to encrypt the entitlement messages (Col. 8, lines 39-44).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 3, 4, 6, 7, 15, 16, 18, 19, 27, 28, 33, 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pinder, U.S. Patent No. 6,105,134, in view of Mniszewski, U.S. Patent No. 4,731,840. Referring to claims 3, 4, 6, 7, 15, 16, 18, 19, 27, 28, 33, 34, Pinder does not disclose an encryption key threshold length. Mniszewski

Art Unit: 2132

discloses a method for encryption and transmission of digital data wherein the DES encryption is used that has 64 bit encryption keys (Col. 1, lines 44-45), which meets the 64 bit threshold limitation. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use DES encryption in the data encryption security module of Heer because DES encryption is the US standard cryptosystem as taught in Mniszewski (Col. 1, lines 31-35).

7. Claims 10, 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pinder, U.S. Patent No. 6,105,134, in view of Tatebayashi, U.S. Patent No. 5,124,117. Referring to claims 10, 22, Pinder does not disclose that the computed keys could be a Diffie-Hellman key. Tatebayashi discloses a cryptographic key distribution system that uses DES encryption standards and Diffie-Hellman keys (Col. 2, lines 21-68). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use Diffie-Hellman keys in the data encryption module of Heer in order to provide secure communications as taught in Tatebayashi (Col. 1, lines 26-38).

Allowable Subject Matter

8. Claims 11, 12, 23, 24, 29, 35 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter: The prior art does not disclose using the hash of an internal key and network device identifier, specifically a software serial number, as a key extension.

Conclusion

Art Unit: 2132

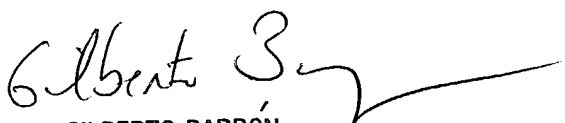
9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E Lanier whose telephone number is 703-305-7684. The examiner can normally be reached on M-Th 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703)305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Benjamin E. Lanier



GILBERTO BARRÓN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100